UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,351	12/11/2001	Howard G. Pinder	A-7274	8293

5642 7590 03/19/2009

SCIENTIFIC-ATLANTA, INC.
INTELLECTUAL PROPERTY DEPARTMENT
5030 SUGARLOAF PARKWAY
LAWRENCEVILLE, GA 30044

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
03/19/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOmail@sciatl.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/015,351
Filing Date: December 11, 2001
Appellant(s): PINDER ET AL.

Randy R. Schen
Reg. No. 62,440
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 01/05/2009 appealing from the Office action mailed 07/08/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,141,530	Rabowsky	10-2000
2002/0114453	Bartholet et al.	08-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 55-76, 83-91 and 105-124 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rabowsky (6,141,530) in view of Bartholet et al (2002/0114453 A1).

Regarding claims 55, 58, 69, 83, 105, 110, 115 and 120, Rabowsky discloses: A method for providing a subscriber of a subscriber network with a program, the subscriber network including a headend with a plurality of receivers coupled thereto, at the headend the method comprising the steps of:

receiving a first ciphertext packet (see, for example, col. 1, lines 53-60; col. 3, lines 5-7; col. 5, lines 62-65);

applying a cryptographic algorithm with a key to the packet to convert the packet to a second ciphertext packet received at the headend (see, for example, col. 3, lines 60-65; col. 4, lines 20-25);

transmitting the second ciphertext packet (see, for example, col. 4, lines 33-41; col. 5, line 62-col. 6, line 4); and

an input port adapted for receiving from a headend of the subscriber network a first ciphertext packet having multiple layers of encryption thereon at the receiver and the encryption keys (see, for example, Fig. 2; col. 2, lines 62-65; col. 3, lines 33-35,

where the cinema files are encrypted at the headend; col. 4, lines 21-32, where a Triple DES encryption may be applied to the cinema file at the headend which corresponds to the recited multiple layers of encryption; col. 8, lines 51-62; col. 9, lines 3-11; since the cinema files transmitted to the theater are encrypted, it is obvious that encryption keys are also transmitted to the theater to be used for decryption process);

a storage device in communication with the cryptographic device adapted to store the ciphertext packet and the keys (see, for example, col. 8, lines 51-62; col. 10, lines 12-25).

Rabowsky, however, does not expressly disclose a scheme to have a key generator adapted to generate a key, a cryptographic device in communication with the input port and the key generator and to use cryptographic algorithms to apply further encryption using the generated key to the incoming encrypted packets from headend without first converting them to cleartext packets, in order to convert them into ciphertext packets with one or more layers of encryption.

Bartholet, on the other hand, discloses a system for secure (i.e., a cryptographic system) storage and communication of data (see abstract, [0002] and [0011]) which is functionally similar to the headend of the Rabowsky. Bartholet also discloses the use of in situ key generators to generate keys to be utilized in the encryption/decryption of data (see [0009]). Bartholet further discloses the following limitations of the claims of the instant invention:

applying to the first ciphertext packet a first cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet (see, for example, [0012], lines 9-

22, where at the storage system as one option without decryption, the received encrypted packets are further encrypted with an additional layer of encryption and then stored);

applying to the second ciphertext packet a second cryptographic algorithm to convert the second ciphertext packet to a third ciphertext packet (see, for example, [0022], where multi-layer encryption are also employed).

Thus, Bartholet teaches a system that is capable of generating keys for further encrypting the already encrypted packets with additional layers of encryption.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the scheme of encryption taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets with additional layers (i.e., multi-layer) of encryption without first decrypting them to produce ciphertext packets with multiple layers of encryption. This scheme may be applied either at the headend or at the theater location (i.e., subscriber location). The deployment of teachings of Bartholet in the system of Rabowsky would raise the cost of the known-plaintext attack and further it would enhance the conventional methods of key management by employing in situ key generators (see Bartholet, [0008]-[0009]).

Regarding claim 56, Rabowsky in view of Bartholet discloses:

wherein the second ciphertext packet corresponds to a cleartext packet that was encrypted using a second cryptographic algorithm (see, for example, Bartholet, [0010], [0022], [0029] and [0035]).

Regarding claims 57, 64, 74, 76, 87, 89, 112 and 122, Rabowsky in view of Bartholet discloses:

wherein the third cryptographic algorithm is a 3DES algorithm (see, for example, col. 4, lines 20-32).

Regarding claim 59, Bartholet discloses:

wherein the first layer of encryption corresponds to applying a second cryptographic algorithm to convert a cleartext packet to a third ciphertext packet (see, for example, page 94, Fig. 4.1(b), encryption operation).

Regarding claims 60, 62, 71, 72 and 86, Rabowsky in view of Bartholet discloses:

wherein the first cryptographic algorithm is a DES algorithm (see, for example, col. 4, lines 20-32).

Regarding claims 61, 63, 70, 73 and 75, Bartholet discloses:

wherein the second layer of encryption corresponds to applying a third cryptographic algorithm to convert the third ciphertext packet to the first ciphertext packet (see, for example, page 94, Fig. 4.1(b), decryption operation).

Regarding claims 65, 90, 108, 113, 118 and 123, Rabowsky in view of Bartholet discloses:

converting the cleartext packet from a first format to a second format (see, for example, col. 2, lines 51-62; col. 3, line 9-15).

Regarding claims 66, 91, 109, 114, 119 and 124, Rabowsky in view of Bartholet discloses:

wherein the first format is an MPEG format (see, for example, col. 4, lines 6-10).

Regarding claims 67, 88, 107, 111, 117, and 121, Rabowsky in view of Bartholet discloses:

receiving at least one key associated with the first ciphertext packet; and applying a third cryptographic algorithm with the at least one key and the encrypt key to convert the third ciphertext packet to a cleartext packet (see, for example, Rabowsky, col. 9, line 65-col. 10, line 10; Bartholet, [0028] and [0029]).

Regarding claim 68, Rabowsky in view of Bartholet discloses:

generating an encryption key at the receiver, wherein the encryption key is applied to the second ciphertext packet with the second cryptographic algorithm (see, for example, col. 11, lines 47-53).

Regarding claim 84, Rabowsky in view of Bartholet discloses:

wherein the third ciphertext packet is stored in a device external to the receiver (see, for example, Fig. 2, storage media 78).

Regarding claim 85, Rabowsky in view of Bartholet discloses:

wherein the third ciphertext packet is stored in an internal storage device of the receiver (see, for example, col. 10, lines 13-15).

Regarding claims 106 and 116, Rabowsky in view of Bartholet discloses:

wherein the receiver is remote from the headend and located at a subscriber location; and further including the step of: storing the third ciphertext packet and the first, second and third keys at the subscriber location (see, for example, col. 1, lines 60-67; col. 8, lines 42-67).

(10) Response to Argument

10.1 With respect to the independent claim 55, appellants, on pages 8 and 9 of the Appeal Brief, argue that: the Office Action fails to even allege that the cited references teach "receiving a first ciphertext packet having multiple layers of encryption thereon at the receiver"... Appellants respectfully submit that encrypting received packets with multi-layer encryption is not the same as "receiving a first ciphertext packet having multiple layers of encryption thereon".

Examiner respectfully disagrees and asserts that Rabowsky discloses that for the security purpose and preventing piracy, the packets are encrypted before transmission from one location to another location (see Abstract, secure electronic delivery; col. 3, lines 5-7; col. 3, lines 18-21). This indicates that the packets are encrypted at least one time (i.e., one layer) before being transmitted and received already encrypted at the

next location (i.e., headend or at the theater system). Rabowsky also discloses that the encryption technology of Triple DES may be implemented for the encryption of the cinema files (see col. 4, lines 20-30). If Rabowsky applies the Triple DES encryption to the packets at the location of the creator (i.e. provider) of the packets or at the headend location then the created cyphertext would be transmitted from the creator location or from the headend in a multi-layer encryption form, because the Triple DES encryption is a kind of multiple encryption operation that encrypts data three times. Furthermore, if as another alternative the multi-layer encryption technique taught by Bartholet for storage and distribution of data (see paragraphs [0011], [0012], lines 9-22 and [0022]) is applied to the packets, for example, at the headend of the Rabowsky's system, the packets that are received at the theater location would have multiple layers of encryption thereon.

Therefore, based on the above submission Rabowsky either alone or in combination with Bartholet teaches that the packets as one option arrive either at the headend or at a subscriber location (i.e., theater system or a regular user) having multiple layer of encryption thereon.

Examiner respectfully submit that a person having ordinary skill in the art would be motivated to implement either a Triple DES encryption of the packets taught by the Rabowsky or combine the multi-layer encryption taught by Bartholet with the teaching of Rabowsky in order to enhance the protection of packets having stronger encryption and to prevent piracy of the cinema files (see Rabowsky, col. 3, lines 18-21 and col. 4, lines 20-30 and Bartholet, [0009]).

10.2 With respect to the independent claim 55, appellants, on page 12 of the Appeal Brief, further argue that: In contrast, *Bartholet* teaches away from such systems and methods, as highlighted belo

in the referenced paragraph "portions" from *Bartholet.*

Examiner respectfully disagrees and asserts that claims 55, 69 and 83 do not recite that the encryption keys are transferred to the headend and to the receiver (i.e., theater system or a subscriber). In this case the teaching of Bartholet can be easily implemented in the system of Rabowsky to generate keys by the in situ key generators at the creator of packets, headend and theater system locations in order to further encrypt the received encrypted packets with more layers of encryptions. On the other hand, according to the independent claims 105, 110, 115 and 120, keys are transferred from the headend to a receiver in addition to the already multi-layer encrypted packets. In this case based on the teaching of Rabowsky the Triple DES scheme can be used to create multi-layer encrypted packets at the headend. Then the multi-layer encrypted packets are transferred to the receiver along with the encryption keys utilized by the Triple DES scheme. Because it is obvious that if there is a need to decrypt the received packets, the applied keys at the headend would be needed at the receiver location. The teaching of Bartholet can be implemented in the system of Rabowsky to generate a new key to be applied to the received multi-layer encrypted packets at the receiver location to add another encryption layer to the packets without first converting them to cleartext packets.

10.3 With respect to the independent claims 69, 83, 105, 110, 115 and 120, appellants present the same arguments presented for claim 55. Therefore, the responses submitted above under 10.1 and 0.2 are similarly applied.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Abdulhakim Nobahar/

Examiner, Art Unit 2432

March 13, 2009

Conferees:

Kambiz Zand

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434

Andrew Nalven

/Andrew L Nalven/

Primary Examiner, Art Unit 2434